UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,621	04/26/2001	Harald Vater	JEK/YATER	8124

23364 7590 05/13/2008

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte HARALD VATER and HERMANN DREXLER

Appeal 2008-0134
Application 09/763,621
Technology Center 2100

Decided: May 13, 2008

Before HOWARD B. BLANKENSHIP, ST. JOHN COURTENAY III, and STEPHEN C. SIU, *Administrative Patent Judges*.

BLANKENSHIP, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-18, which are all the claims in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Appellants' invention relates to a data carrier (e.g., a "smart card") having a semiconductor chip and memory in which data and operations are disguised to prevent unauthorized access to the data. (*See* Abstract; Spec. 1.) Claim 1 is illustrative.

1. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that

the operation (h) is disguised before its execution to obtain a disguised operation (h_{RI}) that is a different operation than the operation (h),

the disguised operation (h_{RI}) is executed with disguised input data, and

the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{RI}) with disguised input data yields output data (y) identical with the output data (y) determined upon execution of the operation (h) with input data (x),

whereby disguising operation (h) prevents analysis of said operation (h) and exposure of secret information about said semiconductor chip should a potential attacker intercept signal patterns generated during execution of said disguised operation (h_{RI}).

The Examiner relies on the following reference as evidence of unpatentability.

Kocher	US 2001/0053220 A1	Dec. 20, 2001

Claims 1-18 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Kocher.

The Examiner applies Kocher to instant claim 1 in the rejection set forth at pages 3 and 4 of the Answer.

Appellants in the Appeal Brief submit that Kocher fails to disclose an operation (h) that is disguised before its execution to obtain a disguised operation (h_{RI}) that is "a different operation than" the operation (h), as recited in claim 1. According to Appellants, Kocher teaches use of a Data Encryption Standard (DES) algorithm, but not a disguised version of the standard algorithm. In Appellants' view, there is no attempt to disguise operations because Kocher teaches only "standard" DES operations.

Appellants thus contest the Examiner's finding with respect to the teachings of the reference. What a reference teaches is a question of fact. *In re Baird*, 16 F.3d 380, 382 (Fed. Cir. 1994); *In re Beattie*, 974 F.2d 1309, 1311 (Fed. Cir. 1992).

Kocher describes an "improved" implementation of DES by introducing additional random state information into the cryptographic processing. The random state information is mixed with the keys, plaintext messages, and intermediate quantities used during processing. Kocher ¶ [0009]. The reference teaches that the standard DES algorithm involves three primary types of operations: permutations, S lookups, and bitwise XORs. ¶ [0011]. In Kocher's system, for the S table lookup operations, the S tables themselves are stored in the device's memory in "blinded" form, such that the S table inputs and outputs are blinded with random values. The S tables are blinded and randomly permuted, and are periodically re-shuffled. *Id.*

The process of loading a key or message into a standard DES implementation can leak information about the key or plaintext. As Appellants acknowledge, Kocher teaches disguising of input data. The inputs to the DES function (the plaintext and the key, when encrypted) are encoded in a different form than usual. Kocher ¶ [0033]; *see also* ¶ ¶ [0034] - [0035].

However, the reference also teaches that Kocher's "leak-minimizing" DES implementation modifies the initialization and updating of the S tables to contribute against external monitoring attacks. The tables are, preferably, initialized with unique random parameters. Kocher ¶ ¶ [0039] - [0047]. The tables are also, preferably, updated with random bits. ¶ [0048] - [0049]. As the Examiner notes, Kocher claims masking a table lookup operation. Kocher p. 10, claim 37. The Examiner also refers to paragraph [0036] of Kocher, which indicates comparison of the "leak-minimizing" DES implementation to quantities that would have been produced "by a standard DES protocol."

We are thus not persuaded that Kocher is limited to describing only "standard" DES operations. In our view, Kocher provides ample support for the contested finding of the Examiner.

We have considered all of Appellants' arguments presented in the briefs but are not persuaded of error in the Examiner's finding of anticipation with respect to claim 1. Claims 2 through 18 fall with claim 1, because the claims have not been separately argued. *See* 37 C.F.R. § 41.37(c)(1)(vii).

CONCLUSION

The rejection of claims 1-18 under 35 U.S.C. § 102(e) as being anticipated by Kocher is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED

rwk

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA VA 22314